UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,112	06/19/2002	Masayuki Hatanaka	020231	3705

38834 7590 12/16/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/069,112	HATANAKA ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) *46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/27/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: section heading such as "Background Art", Disclosure of the Invention", Summary etc. should appear in upper case, without underline or bold type. Applicant is also reminded to follow the correct order of the sections and to choose correct section headings.

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1 – 45 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 9 of U.S. Patent No. 6,898,708. Although the conflicting claims are not identical, they are not patentably distinct from each other because in the instant case all elements of claims 1 – 45 correspond to

claims 1 – 9 of U. S. Patent No. 6,898,708, except in the instant claims 1, 7, 12, 19 30, 42 and 44 the element, symmetric key is referred in claims 1 and 6 of the Patent as private key. It would have been obvious to one having ordinary skill in the art to recognize that the symmetric key is equivalent to the private key, as symmetric key is single-key and private key.

3. Claim 1 – 45 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 22 of copending Application No. 10069118. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/features of claimed data distribution system of instant application exist in copending application in similar or different names, essentially performing same tasks. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

4. Claim 1 – 45 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 25 of copending Application No. 10130301. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/features of claimed data distribution system of instant application exist in copending application in similar or different names, essentially performing same tasks. This is a provisional

obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

5. Claim 1 – 45 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 23 of copending Application No. 10129960. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/features of claimed data distribution system of instant application exist in copending application in similar or different names, essentially performing same tasks. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

6. Claim 1 – 45 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 36 of copending Application No. 10148178. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/features of claimed data distribution system of instant application exist in copending application in similar or different names, essentially performing same tasks. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

7. Claim 1 – 45 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 39 of copending Application No. 10130302. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/features of claimed data distribution system of instant application exist in copending application in similar or different names, essentially performing same tasks. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

8. Claim 1 – 45 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 18 of copending Application No. 10069113. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/features of claimed data distribution system of instant application exist in copending application in similar or different names, essentially performing same tasks. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1- 45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform with current U.S. Practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

For example, Claims 31 and 42 recite, "...releasably attached ...". The examiner will interpret the claims as best understood for applying the appropriate art for rejection purposes.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 1 – 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi et al. (U.S. Patent Number 5,124,117) in view of Misra et al. (U.S. Patent Number 6,189,146) .

11. Regarding Claim 1, Tatebayashi discloses a first interface unit (350) for externally transmitting data;

a first session key generating unit (314) for producing a first symmetric key to be updated in response to every transmission of said license key (Tatebayashi Summary and Column 12 lines 16 – 35);

a session key encryption processing unit (316) for encrypting said first symmetric key with a first public encryption key, and applying the encrypted first symmetric key to said first interface unit (Tatebayashi Summary and Column 12 lines 16 – 35);

a session key decrypting unit (318) for decrypting a second symmetric key and a second public encryption key returned after being encrypted with said first symmetric key based on said first symmetric key to extract said second symmetric key and said second public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35);

a first license data encryption processing unit (320) for encrypting said license key with said second public encryption key extracted by said session key decrypting unit (Tatebayashi Summary and Column 12 lines 16 – 35); and

a second license data encryption processing unit (822) for further encrypting the output of said first license data encryption processing unit with said second symmetric key extracted by said session key decrypting unit, and supplying the encrypted output to said first interface unit (Tatebayashi Summary and Column 12 lines 16 – 35), wherein each of said terminals includes:

a second interface unit for externally transmitting the data (Tatebayashi Summary and Column 12 lines 16 – 35), and

a data storing unit (140) for receiving and storing at least said license key from said content data supply device (Tatebayashi Summary and Column 12 lines 16 – 35);

said first public encryption key is predetermined for said data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35); and said data storing unit includes:

a first key holding unit (1402) for holding a first private decryption key for decrypting the data encrypted with said first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35),

a first decryption processing unit (1404) for receiving and decrypting said first symmetric key encrypted with said first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35),

a second key holding unit (1405) for holding said second public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35),

a second session key generating unit (1432) for producing said second symmetric key, a first encryption processing unit (1406) for encrypting said second

public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said second interface unit, a second decryption processing unit (1410) for receiving said license key encrypted with said second symmetric key, further encrypted with said second public encryption key and applied from said second license data encryption processing unit, and decrypting the received license key based on said second symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third key holding unit (1415) for holding a second private decryption key used for decrypting the data encrypted with said second public encryption key and being unique to said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third decryption processing unit (1416) for receiving said license key encrypted with said second public encryption key, and decrypting the received license key with said second private decryption key for extraction (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a memory unit (1412) for storing said encrypted content data and said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi

teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

12. Regarding Claim 7, Tatebayashi discloses an interface unit (350) for externally transmitting data;

a session key generating unit (314) for producing a first symmetric key to be updated in response to every transmission of said license key (Tatebayashi Summary and Column 12 lines 16 – 35);

a session key encryption processing unit (316) for encrypting said first symmetric key with a first public encryption key predetermined corresponding to said data storing unit of said user terminal, and applying the encrypted first symmetric key to said interface unit (Tatebayashi Summary and Column 12 lines 16 – 35);

a session key decrypting unit (318) for decrypting and extracting a second symmetric key and a second public encryption key returned after being encrypted with said first symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35);

a first license data encryption processing unit (320) for encrypting said license key for decrypting said encrypted content data with said second public encryption key

decrypted by said session key decrypting unit (Tatebayashi Summary and Column 12 lines 16 – 35); and

a second license encryption processing unit (322) for further encrypting the output of said first license data encryption processing unit with said second symmetric key, and applying the encrypted output to said interface unit for supply to each of said terminals (Tatebayashi Summary and Column 12 lines 16 – 35).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

13. Regarding Claim 12, Tatebayashi discloses an interface unit (350) for transmitting data to and from said recording device;

a connecting unit (2010, 2030) for connecting said interface unit and said recording device for supply of the data (Tatebayashi Summary and Column 12 lines 16 – 35);

a first session key generating unit (314) for producing a first symmetric key to be updated in response to every supply of said license key (Tatebayashi Summary and Column 12 lines 16 – 35);

a session key encryption processing unit (316) for encrypting said first symmetric key with a first public encryption key predetermined corresponding to said recording device, and applying the encrypted first symmetric key to said interface unit (Tatebayashi Summary and Column 12 lines 16 – 35);

a session key decrypting unit (318) for decrypting and extracting a second symmetric key and a second public encryption key applied from the recording device connected to said connecting unit after being encrypted with said first symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35);

a first license data encryption processing unit (320) for encrypting said license key for decrypting said encrypted content data with said second public encryption key decrypted by said session key decrypting unit (Tatebayashi Summary and Column 12 lines 16 – 35); and

a second license encryption processing unit (322) for further encrypting the output of said first license data encryption processing unit with said second symmetric key, and applying the encrypted output to said interface unit for supply to said recording device connected to the connecting unit (Tatebayashi Summary and Column 12 lines 16 – 35).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption

key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

14. Regarding Claim 19, Tatebayashi discloses a first interface unit for externally transmitting data; and a data storing unit (140) for receiving and storing said license key (Tatebayashi Summary and Column 12 lines 16 – 35), wherein said data storing unit includes:

a first key holding unit (1402) for holding a first private decryption key for decrypting the data encrypted with a first public encryption key, a first decryption processing unit (1404) for receiving and decrypting a first symmetric key encrypted with said first public encryption key and externally input, a second key holding unit (1405) for holding a second public encryption key unique to said data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a second session key generating unit (1432) for producing a second symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35),

a first encryption processing unit (1406) for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said first interface unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a second decryption processing unit (1410) for receiving the license key encrypted with said second public encryption key and further encrypted with said second symmetric key, and decrypting the received license key based on said second symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35),

a third key holding unit (1415) for holding a second private decryption key used for decrypting the data encrypted with said second public encryption key and being unique to said data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a memory unit (1412) for receiving the output of said second decryption processing unit, and storing said license key encrypted with said second public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35), and

a third decryption processing unit (1416) for receiving the license key encrypted with said second public encryption key stored in said memory unit, and decrypting the received license key with said second private decryption key (Tatebayashi Summary and Column 12 lines 16 – 35).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi

teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

15. Regarding Claim 30, Tatebayashi discloses a first interface unit for externally transmitting data; and a data storing unit (140) for receiving and storing said license key (Tatebayashi Summary and Column 12 lines 16 – 35), wherein said data storing unit includes:

a first key holding unit (1402) for holding a first private decryption key for decrypting the data encrypted with a first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35),

a first decryption processing unit (1404) for receiving and decrypting a first symmetric key encrypted with said first public encryption key and externally input (Tatebayashi Summary and Column 12 lines 16 – 35),

a second key holding unit (1405) for holding a second public encryption key unique to said data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a second session key generating unit (1432) for producing a second symmetric key, a first encryption processing unit (1406) for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and

outputting the encrypted keys to said first interface unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a second decryption processing unit (1410) for receiving the license key encrypted with said second public encryption key and further encrypted with said second symmetric key, and decrypting the received license key based on said second symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third key holding unit (1415) for holding a second private decryption key used for decrypting the data encrypted with said second public encryption key and being unique to said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third decryption processing unit (1416) for receiving said license key encrypted with said second public encryption key, and decrypting the received license key with said second private decryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a memory unit (1412) for receiving the output of said third decryption processing unit, and storing said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi

teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

16. Regarding Claim 42, Tatebayashi discloses a first interface unit for transmitting data to and from said data supply device;

a content reproducing unit (Tatebayashi Summary and Column 12 lines 16 – 35); and

a second interface unit for connection to a data storing unit releasably attached to said terminal device (Tatebayashi Summary and Column 12 lines 16 – 35), wherein said content reproducing unit includes:

a fourth key holding unit (1520) for holding a third private decryption key used for decrypting the data encrypted with a third public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35),

a fourth decryption processing unit (1522) for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a third session key generating unit (1502) for producing a third symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35),

a second encryption processing unit (1504) for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35),

a fifth decryption processing unit (1506) for decrypting and extracting the license key encrypted with said third symmetric key in said data storing unit, and a data reproducing unit (1508) for decrypting the encrypted content data recorded in said recording unit with the extracted license key to reproduce the content data (Tatebayashi Summary and Column 12 lines 16 – 35).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

17. Regarding Claim 44, Tatebayashi discloses an interface unit for externally transmitting data;

a memory unit (1412) for recording the data (Tatebayashi Summary and Column 12 lines 16 – 35); and

a parallel data bus (BS3) having a width of m bits (m is a natural number larger than 1 (m > 1)), and transmitting the data between said interface unit and said recording unit (Tatebayashi Summary and Column 12 lines 16 – 35), wherein said interface unit includes:

a plurality of terminals (1462.0 - 1462.3) (Tatebayashi Summary and Column 12 lines 16 – 35),

selecting means for selecting a predetermined terminals) of one or n in number (n is a natural satisfying (1 < n <= m)) as a terminal(s) for externally receiving data in accordance with a switching instruction for a bit width of the externally applied input data (Tatebayashi Summary and Column 12 lines 16 – 35),

first converting means for operating in accordance with said switching instruction to convert serial data externally applied via said selected one terminal or parallel data of an n-bit width externally applied via said n terminals into parallel data of an m-bit width, and supply the converted parallel data to said parallel data bus (Tatebayashi Summary and Column 12 lines 16 – 35), and

second converting means for converting the parallel data of the m-bit width applied from said parallel data bus into serial data, and externally outputting the

converted serial data via predetermined one terminal among said plurality of terminals (Tatebayashi Summary and Column 12 lines 16 – 35);

a first key holding unit (1402) for holding a first private decryption key for decrypting data encrypted with a first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35);

a first decryption processing unit (1404) for receiving a first symmetric key encrypted with said first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35), and

decrypting the received first symmetric key based on said first private decryption key (Tatebayashi Summary and Column 12 lines 16 – 35);

a second key holding unit (1405) for holding a second public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

a session key generating unit (1432) for producing a second symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

a first encryption processing unit (1406) for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said interface unit via said parallel data bus (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

a second encryption processing unit (1410) for receiving a license key encrypted with said second public encryption key, and further encrypted with said second symmetric key, and decrypting the received license key based on said second symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

a third key holding unit (1415) for holding a second private decryption key set uniquely to said recording device for decrypting the data encrypted with said second public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

a third decryption processing unit (1416) for receiving the license key encrypted with said second public encryption key, and decrypting the received license key based on said second private decryption key to extract said license key, wherein said recording unit stores said encrypted content data and said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

Tatebayashi does not explicitly disclose storing license key. However, Misra discloses a licensing system where the license key is encrypted with a public encryption key and decrypting the license key with private decryption key (Misra Column 11 line 46 – Column 12 line 14). Motivation to combine the invention of Misra with Tatebayashi teachings comes from the need for securing license data with license key. Tatebayashi themselves provide a discussion of the needed license key (classical key) but they do not explicitly state that the classical key can be used as a license key. It would be obvious to one of ordinary skill in the art to combine Misra with Tatebayashi because

security is needed for encrypting the license data for the distribution of data and Misra provides some details of how to secure the license data with license key.

18. Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Tatebayashi discloses wherein each of said terminals further includes a content reproducing unit; said content reproducing unit includes: a fourth key holding unit (1520) for holding a third private decryption key used for decrypting the data encrypted with said third public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a fourth decryption processing unit (1522) for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third session key generating unit (1502) for producing a third symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a second encryption processing unit (1504) for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a fifth decryption processing unit (1506) for decrypting and extracting said license key encrypted based on said third symmetric key in said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a data reproducing unit (1508) for receiving said encrypted content data recorded in said memory unit from said data storing unit, and decrypting said encrypted content data with said extracted license key for reproduction (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); said data storing unit further includes:

a third encryption processing unit (1430) for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said data storing unit sends instructions to receive by said content reproducing unit said third symmetric key encrypted with said second symmetric key, to encrypt by said first encryption processing unit said license key stored in said memory unit with said third symmetric key decrypted and extracted based on said second symmetric key by said second decryption processing unit (1410), and to output the encrypted license key to said content reproducing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

19. Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Tatebayashi discloses a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key of a different data storing unit in a transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a fourth encryption processing unit (1414) for performing the encrypting processing with the second public encryption key of said different data storing unit; said second session key generating unit generates said second symmetric key in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said fourth encryption processing unit encrypts said license key stored in said memory unit with the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said fourth symmetric key, and outputs the encrypted output to said

different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

20. Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Tatebayashi discloses transfer accepting processing of said data storing unit for receiving said license key transferred from said different data storing unit in accordance with transfer processing of said different data storing unit is performed such that:

said first decryption processing unit decrypts and extracts said second symmetric key encrypted with said first public encryption key and generated by said different data storing unit in said transfer acceptance processing (Tatebayashi Summary and Column 12 lines 16 – 35),

said second session key generating unit generates said fourth symmetric key in accordance with said transfer acceptance processing (Tatebayashi Summary and Column 12 lines 16 – 35),

said first encryption processing unit encrypts said second public encryption key and said fourth symmetric key with said second symmetric key for output the encrypted keys in accordance with said transfer acceptance Processing (Tatebayashi Summary and Column 12 lines 16 – 35), and

said second decryption processing unit decrypts with said fourth symmetric key the license key encrypted with said second public encryption key of said different data storing unit, and further encrypted with said fourth symmetric key (Tatebayashi Summary and Column 12 lines 16 – 35).

21. Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Tatebayashi discloses said memory unit receives the output of said second decryption processing unit, and stores said license key encrypted with said second public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35), and

said third decryption processing unit decrypts said license key encrypted with said second public encryption key stored in said memory unit with said second private decryption key (Tatebayashi Summary and Column 12 lines 16 – 35).

22. Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Tatebayashi discloses said third decryption processing unit receives the output of said second decryption processing unit, and decrypts said license key encrypted with said second public encryption key with said second private decryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

said memory unit receives the output of said third decryption processing unit, and stores said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

23. Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Tatebayashi discloses said first public encryption key is applied from said terminal via said interface unit (Tatebayashi Summary and Column 12 lines 16 – 35), and

said session key encryption processing unit encrypts said first symmetric key with said applied first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35).

24. Claim 9 is rejected as applied above in rejecting claim 7. Furthermore, Tatebayashi discloses said data supply device further includes:

an authentication key holding unit for holding an authentication key,

an authentication decryption processing unit (326) for decrypting and extracting authentication data being decodable with said authentication key, obtained from said terminal via said interface unit and predetermined for said data storing unit of said terminal (Tatebayashi Summary and Column 12 lines 16 – 35), and

a control unit (312) for performing authentication processing based on said authentication data extracted by said authentication decryption processing unit, and determining whether at least the license key is to be supplied to the terminal providing said obtained authentication data or not (Tatebayashi Summary and Column 12 lines 16 – 35).

25. Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Tatebayashi discloses said first public encryption key is obtained from each of said terminals via said interface unit after being encrypted together with said authentication data into a form decodable with said authentication key (Tatebayashi Summary and Column 12 lines 16 – 35), and

said authentication data decryption processing unit decrypts with said authentication key said authentication data and said first public encryption key obtained via said interface unit and encrypted into a form decodable with said authentication key, extracts said authentication data and said first public encryption key, and outputs said extracted authentication data and said extracted first public encryption key to said control unit and said session key encryption processing unit, respectively (Tatebayashi Summary and Column 12 lines 16 – 35).

26. Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Tatebayashi discloses said data supply device includes:

an encryption key holding unit for holding a terminal common encryption key for performing encryption allowing decryption in each of said terminals (Tatebayashi Summary and Column 12 lines 16 – 35), and

a third license encryption processing unit for encrypting said license key with said terminal common encryption key held in said encryption key holding unit, and outputting the encrypted license key to said first license encryption processing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

27. Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Tatebayashi discloses each of said recording devices is a memory card, and said recording device can be directly connected to said memory card (Tatebayashi Summary and Column 12 lines 16 – 35).

28. Claim 14 is rejected as applied above in rejecting claim 12. Furthermore, Tatebayashi discloses said first public encryption key is applied from each of said recording devices via said interface unit, and said session key encryption processing unit encrypts said first symmetric key with said applied first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35).

29. Claim 15 is rejected as applied above in rejecting claim 12. Furthermore, Tatebayashi discloses an authentication decryption processing unit (326) for decrypting and extracting authentication data being decodable with an authentication key, and obtained from said recording device via said interface unit (Tatebayashi Summary and Column 12 lines 16 – 35), and

a control unit (312) for performing authentication processing based on said authentication data extracted by said authentication decryption processing unit, and determining whether at least the license key is to be output to said recording device or not (Tatebayashi Summary and Column 12 lines 16 – 35).

30. Claim 16 is rejected as applied above in rejecting claim 12. Furthermore, Tatebayashi discloses said first public encryption key is obtained from said recording devices via said interface unit after being encrypted together with said authentication data into a form decodable with said authentication key (Tatebayashi Summary and Column 12 lines 16 – 35), and

said authentication data decryption processing unit decrypts with said authentication key said authentication data and said first public encryption key obtained via said interface unit and encrypted into a form decodable with said authentication key, extracts said authentication data and said first public encryption key, and outputs said extracted authentication data and said extracted first public encryption key to said control unit and said session key encryption processing unit, respectively (Tatebayashi Summary and Column 12 lines 16 – 35).

31. Claim 17 is rejected as applied above in rejecting claim 10. Furthermore, Tatebayashi discloses said data supply device includes:

an encryption key holding unit (330) attached to said recording device for obtaining said license key and said encrypted content data stored in said recording device, and holding a terminal common encryption key for performing encryption allowing decryption by a plurality of terminals decrypting said encrypted content data to obtain the content data (Tatebayashi Summary and Column 12 lines 16 – 35), and

a third license encryption processing unit (332) for encrypting said license key based on said terminal common encryption key held in said encryption key holding unit, and outputting the encrypted license key to said first license encryption processing unit (Tatebayashi Summary and Column 12 lines 16 – 35).

32. Claim 18 is rejected as applied above in rejecting claim 12. Furthermore, Tatebayashi discloses said recording device includes means for changing the number of terminals connected to said interface unit for externally receiving the data, and performing switching between a serial mode for performing data communication on a bit-by-bit basis and a parallel mode for performing data communication by multiple bits at a time (Tatebayashi Summary and Column 12 lines 16 – 35);

said data supply device supplies said encrypted content data together with said license key to said recording device via said interface unit (Tatebayashi Summary and Column 12 lines 16 – 35); and

said interface unit instructs the parallel mode to said recording device when at least said encrypted content data is to be input to said recording device (Tatebayashi Summary and Column 12 lines 16 – 35).

33. Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Tatebayashi discloses said data storing unit is a recording device releasably attached to said terminal device (Tatebayashi Summary and Column 12 lines 16 – 35).

34. Claim 21 is rejected as applied above in rejecting claim 19. Furthermore, Tatebayashi discloses said data storing unit further includes a fourth key holding unit (1401) holding said first public encryption key and being capable of externally outputting said first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35).

35. Claim 22 is rejected as applied above in rejecting claim 19. Furthermore, Tatebayashi discloses said data storing unit further includes a first data holding unit (1442) for encrypting and holding said first public encryption key and first authentication data unique to said data storing unit and determined uniquely to said first public encryption key in a form allowing decryption with a predetermined authentication key (Tatebayashi Summary and Column 12 lines 16 – 35)

36. Claim 23 is rejected as applied above in rejecting claim 19. Furthermore, Tatebayashi discloses said terminal device further includes a content reproducing unit; said content reproducing unit includes:

a fifth key holding unit (1520) for holding a third private decryption key used for decrypting the data encrypted with a third public encryption key unique to said content reproducing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a fourth decryption processing unit (1522) for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third session key generating unit (1502) for producing a third symmetric key, a second encryption processing unit (1504) for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption

processing unit, and outputting the encrypted third symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a fifth decryption processing unit (1506) for decrypting and extracting the license key encrypted with said third symmetric key in said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a data reproducing unit (1508) for decrypting the encrypted content data recorded in said recording unit with said extracted license key to reproduce the content data (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said data storing unit further includes a third encryption processing unit (1430) for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit (1410) further receives said third symmetric key encrypted with said second symmetric key in said content reproducing unit, and decrypts said encrypted third symmetric key based on said second symmetric key to extract said third symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said third decryption processing unit decrypts said license key encrypted with said second public encryption key stored in said memory unit based on said second private decryption key, and extracts said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit further encrypts said license key extracted by said third decryption processing unit base; on said third symmetric key extracted by said second decryption processing unit, and applies the encrypted license key to said content reproducing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

37. Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Tatebayashi discloses said content reproducing unit further includes a sixth key holding unit (1524) for holding said third public encryption key, and being capable of externally outputting said third public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

38. Claim 25 is rejected as applied above in rejecting claim 23. Furthermore, Tatebayashi discloses said content reproducing unit includes a second data holding unit (1525) for encrypting and holding said third public encryption key and second authentication data being unique to said data storing unit and determined uniquely with respect to the third public encryption key such that said third public encryption key and said second authentication data can be decrypted with a predetermined authentication key (Tatebayashi Summary and Column 12 lines 16 – 35); said data storing unit further includes:

an authentication key holding unit for holding said authentication key (Tatebayashi Summary and Column 12 lines 16 – 35),

an authentication data decryption processing unit for decrypting said second authentication data applied from said data storing unit based on said authentication key to extract said third public encryption key and said first authentication data (Tatebayashi Summary and Column 12 lines 16 – 35), and

a control unit (1420) for performing authentication based on said second authentication data, and determining whether at least the license key is to be output to said content reproducing unit or not (Tatebayashi Summary and Column 12 lines 16 – 35); and

said authentication data decryption processing unit applies said extracted third public encryption key and said extracted second authentication data to said third encryption processing unit and said control unit, respectively (Tatebayashi Summary and Column 12 lines 16 – 35).

39. Claim 26 is rejected as applied above in rejecting claim 23. Furthermore, Tatebayashi discloses said license key is stored in the memory unit after being encrypted into a form allowing decryption with a terminal common decryption key common to said plurality of terminals (Tatebayashi Summary and Column 12 lines 16 – 35); said content reproducing unit further includes:

a decryption key holding unit for holding said terminal common decryption key (Tatebayashi Summary and Column 12 lines 16 – 35), and

a sixth decryption processing unit for decrypting the output of said fifth decryption processing unit based on said terminal common decryption key to extract said license key.

40. Claim 27 is rejected as applied above in rejecting claim 19. Furthermore, Tatebayashi discloses a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key of a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35), and

a fourth encryption processing unit (1414) for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing (Tatebayashi Summary and Column 12 lines 16 – 35);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key

(Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

41. Claim 28 is rejected as applied above in rejecting claim 21. Furthermore, Tatebayashi discloses a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key applied from a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35), and

a fourth encryption processing unit (1414) for performing the encrypting processing with the second public encryption key of said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second session key generating unit generates said second symmetric key in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key; said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

42. Claim 29 is rejected as applied above in rejecting claim 20. Furthermore, Tatebayashi discloses said data storing unit further includes:

an authentication key holding unit for holding said authentication key (Tatebayashi Summary and Column 12 lines 16 – 35),

an authentication data decryption processing unit for decrypting said first authentication data applied from a different data storing unit based on said authentication key to extract said first public encryption key and said first authentication data in accordance with transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a control unit (1420) for performing authentication based on said first authentication data and in accordance with said transfer processing, and determining whether at least the license key is to be output to said different data storing unit or not (Tatebayashi Summary and Column 12 lines 16 – 35),

a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key output from said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a fourth encryption processing unit (1414) for performing the encrypting processing with the second public encryption key of said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second session key generating unit generates said second symmetric key in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

43. Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Tatebayashi discloses said data storing unit is a recording device releasably attached to said terminal device (Tatebayashi Summary and Column 12 lines 16 – 35).

44. Claim 32 is rejected as applied above in rejecting claim 30. Furthermore, Tatebayashi discloses said data storing unit further includes a fourth key holding unit (1401) holding said first public encryption key and being capable of externally outputting said first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35).

45. Claim 33 is rejected as applied above in rejecting claim 30. Furthermore, Tatebayashi discloses a first data holding unit (1442) for encrypting and holding said first public encryption key and first authentication data unique to said data storing unit and determined uniquely to said first public encryption key in a form allowing decryption with a predetermined authentication key (Tatebayashi Summary and Column 12 lines 16 – 35).

46. Claim 34 is rejected as applied above in rejecting claim 21. Furthermore, Tatebayashi discloses said terminal device further includes a content reproducing unit; said content reproducing unit includes:

a fifth key holding unit (1520) for holding a third private decryption key used for decrypting the data encrypted with a third public encryption key predetermined for said

content reproducing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a fourth decryption processing unit (1522) for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a third session key generating unit (1502) for producing a third symmetric key, a second encryption processing unit (1504) for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

a fifth decryption processing unit (1506) for decrypting and extracting the license key encrypted with said third symmetric key in said data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a data reproducing unit (1508) for decrypting the encrypted content data recorded in said recording unit with said extracted license key to reproduce the content data (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said data storing unit further includes a third encryption processing unit (1430) for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit (1410) further receives said third symmetric key encrypted with said second symmetric key in said content reproducing unit, and decrypts said encrypted third symmetric key based on said second symmetric key to extract said third symmetric key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit further encrypts said license key stored in said memory unit based on said third symmetric key extracted by said second decryption processing unit, and applies the encrypted license key to said content reproducing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

47. Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Tatebayashi discloses said content reproducing unit further includes a sixth key holding unit (1524) for holding said third public encryption key, and being capable of externally outputting said third public encryption key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

48. Claim 36 is rejected as applied above in rejecting claim 34. Furthermore, Tatebayashi discloses said content reproducing unit includes a second data holding unit (1525) for encrypting and holding said third public encryption key and second authentication data being unique to said data storing unit and determined uniquely with respect to the third public encryption key such that said third public encryption key and

said second authentication data can be decrypted with a predetermined authentication key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); said data storing unit further includes:

an authentication key holding unit for holding said authentication key (Tatebayashi Summary and Column 12 lines 16 – 35),

an authentication data decryption processing unit for decrypting said second authentication data applied from said data storing unit based on said authentication key to extract said third public encryption key and said first authentication data (Tatebayashi Summary and Column 12 lines 16 – 35), and

a control unit (1420) for performing authentication based on said second authentication data, and determining whether at least the license key is to be output to said content reproducing unit or not (Tatebayashi Summary and Column 12 lines 16 – 35); and

said authentication data decryption processing unit applies said extracted third public encryption key and said extracted second authentication data to said third encryption processing unit and said control unit, respectively (Tatebayashi Summary and Column 12 lines 16 – 35).

49. Claim 37 is rejected as applied above in rejecting claim 34. Furthermore, Tatebayashi discloses said license key is stored in the memory unit after being encrypted into a form allowing decryption with a terminal common decryption key

common to said plurality of terminals (Tatebayashi Summary and Column 12 lines 16 – 35); said content reproducing unit further includes:

a decryption key holding unit for holding said terminal common decryption key (Tatebayashi Summary and Column 12 lines 16 – 35), and

a sixth decryption processing unit for decrypting the output of said fifth decryption processing unit based on said terminal common decryption key to extract said license key .

50. Claim 38 is rejected as applied above in rejecting claim 30. Furthermore, Tatebayashi discloses a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key of a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

fifth encryption processing unit (1414) for performing the a our encrypting processing with the second public encryption key of said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second session key generating unit generates said second symmetric key in accordance with said. transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14),

said fourth encryption processing unit encrypts said extracted license key stored in said memory unit based on the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

51. Claim 39 is rejected as applied above in rejecting claim 38. Furthermore, Tatebayashi discloses said data storing unit further includes a fourth key holding unit (1401) holding said first public encryption key and being capable of externally outputting said first public encryption key (Tatebayashi Summary and Column 12 lines 16 – 35), and

said third encryption processing unit performs encryption based on said first public encryption key applied from said different data storing unit in accordance with

said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

52. Claim 40 is rejected as applied above in rejecting claim 32. Furthermore, Tatebayashi discloses said data storing unit further includes:

a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key output from a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14), and

a fourth encryption processing unit (1414) for performing the encrypting processing with the second public encryption key of said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second session key generating unit generates said second symmetric key in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

53. Claim 41 is rejected as applied above in rejecting claim 33. Furthermore, Tatebayashi discloses said data storing unit further includes:

an authentication key holding unit for holding said authentication key (Tatebayashi Summary and Column 12 lines 16 – 35),

an authentication data decryption processing unit for decrypting said first authentication data applied from a different data storing unit based on said authentication key to extract said first public encryption key and said first authentication

data in accordance with transfer processing for transferring at least said license key to said different data storing unit (Tatebayashi Summary and Column 12 lines 16 – 35),

a control unit (1420) for performing authentication based on said first authentication data and in accordance with said transfer processing, and determining whether at least the license key is to be output to said different data storing unit or not,

a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key output from said different data storing unit in accordance with said transfer processing (Tatebayashi Summary and Column 12 lines 16 – 35), and

a fourth encryption processing unit (1414) for performing the encrypting processing with the second public encryption key of said different data storing unit (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second session key generating unit generates said second symmetric key in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private

decryption key in accordance with said transfer processing to extract said license key (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14);

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14); and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

54. Claim 43 is rejected as applied above in rejecting claim 42. Furthermore, Tatebayashi discloses a data holding unit (1525) for holding second authentication data and said third public encryption key in a form allowing decryption with an authentication key for external output (Tatebayashi Summary; Column 12 lines 16 – 35 and Column 14 line 55 – Column 15 line 14).

55. Claim 45 is rejected as applied above in rejecting claim 44. Furthermore, Tatebayashi discloses an authentication data holding unit (1442) for holding an authentication data prepared by encrypting said first public encryption key and a

certificate data corresponding to said first public encryption key in a form allowing external decryption with an authentication key for external output (Tatebayashi Summary and Column 12 lines 16 – 35).

Conclusion

56. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the disclosing in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially disclosing all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

57. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

58. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Cel
Primary Examiner
AU 2131
12/9/05

Pramila Parthasarathy
December 03, 2005.